

# UNITED STATES DISTRICT COURT

for the  
Western District of Washington

FILED	LODGED
RECEIVED	
Apr 17 2025	
CLERK U.S. DISTRICT COURT WESTERN DISTRICT OF WASHINGTON AT TACOMA	
BY	DEPUTY

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)  
SUBJECT PREMISES/PERSON

Case No. MJ25-5145

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, incorporated herein by reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. §§ 2251(a), (e), 2252(a)  
(2), (b)(1), 2252(a)(4)(B), (b)(2)

Production/Distribution/Possession of Child Pornography and attempt to commit these offenses

The application is based on these facts:

- ☒ See Affidavit of FBI Special Agent Kyle McNeal, continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.

*Kyle McNeal*  
Applicant's signature

Kyle McNeal, Special Agent, FBI  
Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
- ☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 04/11/2025

*Grady J. Leupold*  
Judge's signature

City and state: Bellevue, Washington

Grady J. Leupold, United States Magistrate Judge  
Printed name and title

**AFFIDAVIT**

STATE OF WASHINGTON )  
 ) ss  
 PIERCE COUNTY )

I, KYLE MCNEAL being duly sworn, depose and state as follows:

**INTRODUCTION**

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), assigned to the Special Agent in Charge in Seattle, Washington. I have been an Agent with the FBI since April 2011. As part of my daily duties as an FBI agent, I investigate criminal violations relating to child exploitation and child pornography including violations of Title 18, United States Code §§ 2251(a), 2252A, 2422, and 2423. I have received training regarding child pornography and child exploitation, and have observed and reviewed numerous examples of child pornography in numerous forms of media, including media stored on digital media storage devices such as computers, iPhones, etc. I have also participated in the execution of numerous search warrants involving investigations of child exploitation and/or child pornography offenses. I am a member of the FBI South Sound Child Exploitation and Human Trafficking Task Force in the Western District of Washington, and work with other federal, state, and local law enforcement personnel in the investigation and prosecution of crimes involving the sexual exploitation of children. As a federal law enforcement officer who is engaged in enforcing criminal laws, I am authorized by law to request this search warrant.

**PURPOSE OF THE AFFIDAVIT**

2. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the following, which are further described in Attachment A:

a. The premises located at 5944 N 12<sup>th</sup> Street, Joint Base Lewis-Chord (JBLM), Washington 98433 (Hereinafter the "SUBJECT PREMISES")

1           b.     The person of JAMES ANDREW DAVIS, date of birth (DOB)  
2     XX/XX/1991 (the SUBJECT PERSON)

3           c.     A 1986 Chevrolet Blazer bearing Washington Plate: CGN9993  
4     (SUBJECT VEHICLE 1)

5           d.     A 2015 Kia Sportage, bearing Washington Plate: BMH3641  
6     (SUBJECT VEHICLE 2).

7           3.     This Affidavit is submitted in support of an application under Rule 41 of  
8     the Federal Rules of Criminal Procedure for a search warrant for the locations  
9     specifically described in Attachment A of this Affidavit and the content of electronic  
10    storage devices located therein for contraband and evidence, fruits, and instrumentalities  
11    of violations or attempted violations of 18 U.S.C. § 2251(a), (e) (Production of Child  
12    Pornography, 18 U.S.C. 2252(a)(2), (b)(1) (Distribution of Child Pornography), and  
13    18 U.S.C. § 2252(a)(4)(B), (b)(2) (Possession of Child Pornography) (the TARGET  
14    OFFENSES), which items are more specifically described in Attachment B of this  
15    Affidavit.

16           4.     The statements contained in this affidavit are based in part on information  
17    provided by U.S. federal law enforcement agents; written reports about this and other  
18    investigations that I have received, directly or indirectly, from other law enforcement  
19    agents; information gathered from the service of administrative subpoenas; the results of  
20    physical and electronic surveillance conducted by law enforcement agents; independent  
21    investigation and analysis by law enforcement agents/analysts and computer forensic  
22    professionals; and my experience, training and background as a Special Agent. Since this  
23    Affidavit is being submitted for the limited purpose of securing a search warrant, I have  
24    not included each and every fact known to me concerning this investigation. I have set  
25    forth only the facts that I believe are necessary to establish probable cause to believe that  
26    contraband and evidence, fruits, and instrumentalities of violations or attempted  
27    violations of the TARGET OFFENSES will be found at the SUBJECT  
28    PREMISES/PERSON/VEHICLES

**SUMMARY OF PROBABLE CAUSE**

5. Leading up to Thursday, April 10, 2025, a FBI WFO Task Force Officer (TFO) was acting in an undercover (UC) capacity as part of the Metropolitan Police Department-Federal Bureau of Investigation (“MPD-FBI”) Child Exploitation Task Force, operating out of a satellite office in Washington, D.C. In that capacity, the UC entered an adult pornography forum website that he was previously a member and has an internal email within the site. Different areas of this site are known to the UC as a place where people meet, discuss, and trade original images of underage children, links containing child pornography, and videos among other things. The UC has been a member of this site for over a year.

6. The UC posted a message under the personal advertisement that read, [REDACTED]  
[REDACTED]  
[REDACTED]” On April 10, 2025, a user using the screen name, “[REDACTED]” (since identified as the SUBJECT PERSON) initiated a private email chat with the UC within the website. The SUBJECT PERSON stated, “you like [REDACTED] stuff? I’m willing to chat.” The SUBJECT PERSON informed the UC that [REDACTED]  
[REDACTED] and asked the UC if he had any pics to trade. The SUBJECT PERSON referred to [REDACTED] at one point, saying, “Same I had her hand caressing me and came on her feet wanna email? Off this?”

7. The SUBJECT PERSON provided his KIK account screen name, “[REDACTED]” and began communicating with the UC via KIK private messenger. The SUBJECT PERSON introduced himself as “James,” a 35-year-old male residing in Oregon with his wife [REDACTED]. He said he has been [REDACTED]  
[REDACTED]. The SUBJECT PERSON told the UC that he has been having sexual contact with [REDACTED] He described the firsttime he sexually abused her as follows: [REDACTED]  
[REDACTED]

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13 [REDACTED] The focus of the images is on the girl's clothed genitals. The SUBJECT  
14 PERSON also sent the UC an image purportedly of [REDACTED]  
15 [REDACTED]

16 [REDACTED] The UC asked the SUBJECT PERSON to send him a live image of  
17 that same vehicle to prove that the child was one that he had access to and not a random  
18 image from the internet. The SUBJECT PERSON complied and sent the UC a live video  
19 of the passenger side of the vehicle which visually matched the photo sent by the  
20 SUBJECT PERSON.

21 10. Based on the context of the chat conversation, it appeared that the  
22 SUBJECT PERSON may have deleted child sexual abuse videos and images [REDACTED]  
23 [REDACTED] after he got caught by her taking a picture of her buttocks.

24 11. The SUBJECT PERSON sent an additional image [REDACTED]  
25 [REDACTED] that shows a male placing his thumb on the bare buttocks of the  
26 female, which appears to further expose her genitals to the camera. The focus of the  
27 image is the female's exposed genitals. According to the SUBJECT PERSON, he took  
this photo [REDACTED] around 4 years ago [REDACTED]. Based on the size of

1 the female in comparison to the male's thumb, lack of pubic hair, and lack of pubic  
2 development, it does appear the female is prepubescent.<sup>1</sup>

3 12. The SUBJECT PERSON informed the UC that [REDACTED]  
4 [REDACTED]  
5 [REDACTED]

6 13. On April 11, 2025, FBI served an Emergency Disclosure Request (EDR) to  
7 Kik re: user [REDACTED] On that same day, Kik responded and provided a registration  
8 email address, [REDACTED]@gmail.com.

9 14. That same day, FBI served an administrative subpoena request on Google  
10 re: email address: [REDACTED]@gmail.com. Google responded IP connection  
11 history that included Comcast IP address 2601:603:177f:33b0:5d61:34db:34:24bf.

12 15. FBI served an EDR to Comcast re: 2601:603:177f:33b0:5d61:34db:34:24bf  
13 on 2025-03-09 at 08:58:26 (a date/time when that a user of the above email address used  
14 that IP address to log into Google's servers). Comcast provided the following subscriber  
15 information verbally for that IP address at that date/time: James Davis with a service  
16 address of 5944 North 12th Street, Lewis McCord, WA 98433. Using commercial  
17 databases, the user of Kik account [REDACTED] is linked to JAMES DAVIS, DOB:  
18 XX/XX/1991.

19 16. According to military records, JAMES DAVIS resides at the SUBJECT  
20 PREMISES with his spouse. Military records indicate [REDACTED]  
21 [REDACTED]  
22 [REDACTED]

23 17. On April 11, 2025, FBI TFO Elijah Allman conducted surveillance at the  
24 SUBJECT PREMISES. In the driveway, TFO Allman observed a Green 1986 Chevrolet  
25 Blazer bearing Washington Plate: CGN9993 (SUBJECT VEHICLE 1). The registered

26 <sup>1</sup> I am aware of the decision in *United States v. Perkins*, 850 F.3d 1109 (9th Cir. 2017). Based on the facts outlined  
27 in this affidavit, I do not believe that case requires that this image be made available to the reviewing magistrate  
judge as part of this application. Should the reviewing magistrate judge believe it is necessary to review this image  
to determine the existence of probable cause, I will make it available upon request.

1 owner of the vehicle was JAMES ANDREW DAVIS. According to Department of  
2 Licensing records, the SUBJECT PERSON is also the registered owner of a 2015 Kia  
3 Sportage, bearing Washington Plate: BMH3641 (SUBJECT VEHICLE 2).z

4 18. Given the SUBJECT PERSON's stated intention [REDACTED]  
5 [REDACTED] as soon as this weekend, potentially (Friday, April 11), federal  
6 law enforcement intends to execute the warrants requested in this application as soon as  
7 possible. I anticipate the execution will begin before 10 pm on Friday, April 11. I am  
8 nonetheless requesting authority to execute this warrant at any time of the day or night to  
9 ensure that federal agents can execute the requested searches as soon as possible once the  
10 necessary operational and staffing resources have been gathered and are ready to  
11 proceed.

12 **BACKGROUND ON CHILD SEXUAL ABUSE MATERIAL,**  
13 **COMPUTERS, AND THE INTERNET**

14 19. I have had both training and experience in the investigation of computer-  
15 related crimes. Based on my training, experience, and knowledge, I know the  
16 following:

17 a. Computers and digital technology are the primary way in which  
18 individuals interested in child pornography interact with each other. Computers  
19 basically serve four functions in connection with child pornography: production,  
20 communication, distribution, and storage.

21 b. Digital cameras and smartphones with cameras save photographs  
22 or videos as a digital file that can be directly transferred to a computer by connecting  
23 the camera or smartphone to the computer, using a cable or via wireless connections  
24 such as "WiFi" or "Bluetooth." Additionally, images and videos taken by a digital  
25 camera or smartphone can be automatically copied to cloud-based storage using either  
26 the wireless network or cellular connection. Images and videos can also be shared  
27 through numerous applications on the smartphone including messages applications,

1 photo-sharing applications, and other image or video based applications. Photos and  
2 videos taken on a digital camera or smartphone may be stored on a removable  
3 memory card in the camera or smartphone. These memory cards are often large  
4 enough to store thousands or tens of thousands of high-resolution photographs or  
5 hundreds of hours of videos.

6 c. A modem allows any computer to connect to another computer  
7 through the use of telephone, cable, or wireless connection. Mobile devices such as  
8 smartphones and tablet computers may also connect to other computers via wireless  
9 connections. Electronic contact can be made to literally millions of computers around  
10 the world. CSAM can therefore be easily, inexpensively, and anonymously (through  
11 electronic communications) produced, distributed, and received by anyone with  
12 access to a computer or smartphone.

13 d. The computer's ability to store images in digital form makes the  
14 computer itself an ideal repository for CSAM. Electronic storage media of various  
15 types—to include computer hard drives, external hard drives, CDs, DVDs, and  
16 “thumb,” “jump,” or “flash” drives, which are very small devices that are plugged into  
17 a port on the computer—can store thousands of images or videos at very high  
18 resolution. It is extremely easy for an individual to take a photo or a video with a  
19 digital camera or camera-bearing smartphone, upload that photo or video to a  
20 computer, and then copy it (or any other files on the computer) to any one of those  
21 media storage devices. Some media storage devices can easily be concealed and  
22 carried on an individual's person. Smartphones and/or mobile phones are also often  
23 carried on an individual's person.

24 e. The Internet affords individuals several different venues for  
25 obtaining, viewing, and trading CSAM in a relatively secure and anonymous fashion.  
26  
27

1 f. Individuals also use online resources to retrieve and store CSAM.  
2 Some online services allow a user to set up an account with a remote computing  
3 service that may provide email services and/or electronic storage of computer files in  
4 any variety of formats. A user can set up an online storage account (sometimes  
5 referred to as “cloud” storage) from any computer or smartphone with access to the  
6 Internet. Even in cases where online storage is used, however, evidence of CSAM  
7 can be found on the user’s computer, smartphone, external media, and across any  
8 (other) device connected to that online storage account, in most cases.

9 g. Based upon my training and experience, I know that users who  
10 possess, receive, distribute, or produce files depicting child sexual abuse material  
11 often transfer these files between their different storage devices and online accounts.  
12 Their reasons for doing so include concealing the files, storing them in one account  
13 versus another account, or having the files accessible to the user on multiple devices.  
14 I am aware of cases where users transferred CSAM files between devices and/or  
15 online accounts, and/or used email or other online messaging accounts to complete the  
16 transfer.

17 h. The use of mobile applications, also referred to as “apps”  
18 continues to be a growing phenomenon related to smartphones and other mobile  
19 computing devices. Apps consist of software downloaded onto mobile devices that  
20 enable users to perform a variety of tasks – such as engaging in online chat, sharing  
21 digital files, reading a book, or playing a game – on a mobile device. Individuals  
22 commonly use such apps to receive, store, distribute, and advertise CSAM, to interact  
23 directly with other like-minded offenders or with potential minor victims, and to  
24 access cloud-storage services where CSAM may be stored.

25 i. As is the case with most digital technology, communications by  
26 way of computer can be saved or stored on the computer used for these purposes.  
27

1 Storing this information can be intentional (*i.e.*, by saving an email as a file on the  
2 computer or saving the location of one's favorite websites in, for example,  
3 "bookmarked" files) or unintentional. Digital information, such as the traces of the  
4 path of an electronic communication, may also be automatically stored in many places  
5 (e.g., temporary files or ISP client software, among others). In addition to electronic  
6 communications, a computer user's Internet activities generally leave traces or  
7 "footprints" in the web cache and history files of the browser used. Such information  
8 is often maintained indefinitely until overwritten by other data.

9 20. Based upon my knowledge, experience, and training in child pornography  
10 investigations, and the training and experience of other law enforcement officers with  
11 whom I have had discussions, I know that there are certain characteristics common to  
12 individuals who have a sexualized interest in children and depictions of children:

13 a. They may receive sexual gratification, stimulation, and satisfaction  
14 from contact with children; or from fantasies they may have viewing children engaged in  
15 sexual activity or in sexually suggestive poses, such as in person, in photographs, or other  
16 visual media; or from literature describing such activity.

17 b. They may collect sexually explicit or suggestive materials in a  
18 variety of media, including photographs, magazines, motion pictures, videotapes, books,  
19 slides, and/or drawings or other visual media. Such individuals often times use these  
20 materials for their own sexual arousal and gratification. Further, they may use these  
21 materials to lower the inhibitions of children they are attempting to seduce, to arouse the  
22 selected child partner, or to demonstrate the desired sexual acts. These individuals may  
23 keep records, to include names, contact information, and/or dates of these interactions, of  
24 the children they have attempted to seduce, arouse, or with whom they have engaged in  
25 the desired sexual acts.

26 c. They often maintain any "hard copies" of child pornographic  
27 material that is, their pictures, films, video tapes, magazines, negatives, photographs,

1 correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of  
2 their home or some other secure location. These individuals typically retain these “hard  
3 copies” of child pornographic material for many years, as they are highly valued.

4 d. Likewise, they often maintain their child pornography collections  
5 that are in a digital or electronic format in a safe, secure and private environment, such as  
6 a computer and surrounding area. These collections are often maintained for several  
7 years and are kept close by, often at the individual’s residence or some otherwise easily  
8 accessible location, to enable the owner to view the collection, which is valued highly.

9 e. They also may correspond with and/or meet others to share  
10 information and materials; rarely destroy correspondence from other child pornography  
11 distributors/collectors; conceal such correspondence as they do their sexually explicit  
12 material; and often maintain lists of names, addresses, and telephone numbers of  
13 individuals with whom they have been in contact and who share the same interests in  
14 child pornography.

15 f. They generally prefer not to be without their child pornography for  
16 any prolonged time period. This behavior has been documented by law enforcement  
17 officers involved in the investigation of child pornography throughout the world.  
18 Importantly, e-mail and cloud storage can be a convenient means by which individuals  
19 can access a collection of child pornography from any computer, at any location with  
20 Internet access. Such individuals therefore do not need to physically carry their  
21 collections with them but rather can access them electronically. Furthermore, these  
22 collections can be stored on email “cloud” servers, which allow users to store a large  
23 amount of material at no cost, and possibly reducing the amount of any evidence of any  
24 of that material on the users’ computer(s).

25 21. Even if such individuals use a portable device (such as a mobile phone) to  
26 access the Internet and child pornography, it is more likely than not that evidence of this  
27 access will be found in his home, the SUBJECT PREMISES, as set forth in Attachment

1 A, including on digital devices other than the portable device (for reasons including the  
2 frequency of “backing up” or “synching” mobile phones to computers or other digital  
3 devices).

4 22. In addition to offenders who collect and store child pornography, law  
5 enforcement has encountered offenders who obtain child pornography from the internet,  
6 view the contents, and subsequently delete the contraband, often after engaging in self-  
7 gratification. In light of technological advancements, increasing Internet speeds and  
8 worldwide availability of child sexual exploitative material, this phenomenon offers the  
9 offender a sense of decreasing risk of being identified and/or apprehended with quantities  
10 of contraband. This type of consumer is commonly referred to as a ‘seek and delete’  
11 offender, knowing that the same or different contraband satisfying their interests remain  
12 easily discoverable and accessible online for future viewing and self-gratification. I  
13 know that, regardless of whether a person discards or collects child pornography he/she  
14 accesses for purposes of viewing and sexual gratification, evidence of such activity is  
15 likely to be found on computers and related digital devices, including storage media, used  
16 by the person. This evidence may include the files themselves, logs of account access  
17 events, contact lists of others engaged in trafficking of child pornography, backup files,  
18 and other electronic artifacts that may be forensically recoverable.

19 23. Given the above-stated facts and based on my knowledge, training and  
20 experience, along with my discussions with other law enforcement officers who  
21 investigate child exploitation crimes, I believe that the SUBJECT PERSON, likely  
22 resides at the SUBJECT PREMISES and likely has a sexualized interest in children and  
23 depictions of children. I therefore believe that the SUBJECT  
24 PREMISES/PERSON/VEHICLES is likely to contain evidence, fruits, and  
25 instrumentalities of the TARGET OFFENSES.

#### 26 **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

27 24. As described above and in Attachment B, this application seeks permission  
to search for evidence, fruits and/or instrumentalities that might be found, in whatever

form they are found. One form in which the evidence, fruits, and/or instrumentalities might be found is data stored on digital devices<sup>2</sup> such as computer hard drives or other electronic storage media.<sup>3</sup> Thus, the warrant applied for would authorize the seizure of digital devices or other electronic storage media or, potentially, the copying of electronically stored information from digital devices or other electronic storage media, all under Rule 41(e)(2)(B).

25. *Probable cause.* Based upon my review of the evidence gathered in this investigation, my review of data and records, information received from other agents and computer forensics examiners, and my training and experience, I submit that if a digital device or other electronic storage media is found during the search of the SUBJECT PREMISES/PERSON/VEHICLES, there is probable cause to believe that evidence, fruits, and/or instrumentalities of the TARGET OFFENSES will be stored on those digital devices or other electronic storage media. As noted above, I believe the SUBJECT PERSON used a digital device at the SUBJECT PREMISES to distribute child sexual abuse imagery he claimed to have created online. There is, therefore, probable cause to believe that evidence, fruits and/or instrumentalities of the TARGET OFFENSES exists and will be found on digital devices or other electronic storage media found in a search of the SUBJECT PREMISES/PERSON/VEHICLES, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be preserved (and consequently also then

---

<sup>2</sup> ["Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

<sup>3</sup> Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

recovered) for months or even years after they have been downloaded onto a storage medium, deleted, or accessed or viewed via the Internet.

Electronic files downloaded to a digital device or other electronic storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a digital device or other electronic storage media, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device or other electronic storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

26. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how digital devices or other electronic storage media were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital devices or other electronic storage media located at the search of the SUBJECT PREMISES/PERSON/VEHICLES because:

- a. Stored data can provide evidence of a file that was once on the digital device or other electronic storage media but has since been deleted or edited, or

1 of a deleted portion of a file (such as a paragraph that has been deleted from a  
2 word processing file). Virtual memory paging systems can leave traces of  
3 information on the digital device or other electronic storage media that show  
4 what tasks and processes were recently active. Web browsers, e-mail  
5 programs, and chat programs store configuration information that can reveal  
6 information such as online nicknames and passwords. Operating systems can  
7 record additional information, such as the history of connections to other  
8 computers, the attachment of peripherals, the attachment of USB flash storage  
9 devices or other external storage media, and the times the digital device or  
10 other electronic storage media was in use. Computer file systems can record  
11 information about the dates files were created and the sequence in which they  
12 were created.

13 b. As explained herein, information stored within a computer and other  
14 electronic storage media may provide crucial evidence of the “who, what, why,  
15 when, where, and how” of the criminal conduct under investigation, thus  
16 enabling the United States to establish and prove each element or alternatively,  
17 to exclude the innocent from further suspicion. In my training and experience,  
18 information stored within a computer or storage media (e.g., registry  
19 information, communications, images and movies, transactional information,  
20 records of session times and durations, internet history, and anti-virus,  
21 spyware, and malware detection programs) can indicate who has used or  
22 controlled the computer or storage media. This “user attribution” evidence is  
23 analogous to the search for “indicia of occupancy” while executing a search  
24 warrant at a residence. The existence or absence of anti-virus, spyware, and  
25 malware detection programs may indicate whether the computer was remotely  
26 accessed, thus inculcating or exculpating the computer owner and/or others  
27 with direct physical access to the computer. Further, computer and storage  
media activity can indicate how and when the computer or storage media was  
accessed or used. For example, as described herein, computers typically  
contain information that log: computer user account session times and  
durations, computer activity associated with user accounts, electronic storage  
media that connected with the computer, and the IP addresses through which  
the computer accessed networks and the internet. Such information allows  
investigators to understand the chronological context of computer or electronic  
storage media access, use, and events relating to the crime under  
investigation.<sup>4</sup> Additionally, some information stored within a computer or  
electronic storage media may provide crucial evidence relating to the physical

---

<sup>4</sup> For example, if the examination of a computer shows that: a) at 11:00am, someone using the computer used an internet browser to log into a bank account in the name of John Doe; b) at 11:02am the internet browser was used to download child pornography; and c) at 11:05 am the internet browser was used to log into a social media account in the name of John Doe, an investigator may reasonably draw an inference that John Doe downloaded child pornography.

1 location of other evidence and the suspect. For example, images stored on a  
2 computer may both show a particular location and have geolocation  
3 information incorporated into its file data. Such file data typically also  
4 contains information indicating when the file or image was created. The  
5 existence of such image files, along with external device connection logs, may  
6 also indicate the presence of additional electronic storage media (e.g., a digital  
7 camera or cellular phone with an incorporated camera). The geographic and  
8 timeline information described herein may either inculcate or exculpate the  
9 computer user. Last, information stored within a computer may provide  
10 relevant insight into the computer user's state of mind as it relates to the  
11 offense under investigation. For example, information within the computer  
12 may indicate the owner's motive and intent to commit a crime (e.g., internet  
13 searches indicating criminal planning), or consciousness of guilt (e.g., running  
14 a "wiping" program to destroy evidence on the computer or password  
15 protecting/encrypting such evidence in an effort to conceal it from law  
16 enforcement).

17 c. A person with appropriate familiarity with how a digital device or other  
18 electronic storage media works can, after examining this forensic evidence in  
19 its proper context, draw conclusions about how the digital device or other  
20 electronic storage media were used, the purpose of their use, who used them,  
21 and when.

22 d. The process of identifying the exact files, blocks, registry entries, logs, or  
23 other forms of forensic evidence on a digital device or other electronic storage  
24 media that are necessary to draw an accurate conclusion is a dynamic process.  
25 While it is possible to specify in advance the records to be sought, digital  
26 evidence is not always data that can be merely reviewed by a review team and  
27 passed along to investigators. Whether data stored on a computer is evidence  
may depend on other information stored on the computer and the application of  
knowledge about how a computer behaves. Therefore, contextual information  
necessary to understand other evidence also falls within the scope of the  
warrant.

e. Further, in finding evidence of how a digital device or other electronic  
storage media was used, the purpose of its use, who used it, and when,  
sometimes it is necessary to establish that a particular thing is not present. For  
example, the presence or absence of counter-forensic programs or anti-virus  
programs (and associated data) may be relevant to establishing the user's  
intent.

**REQUEST FOR AUTHORITY TO CONDUCT OFF-SITE SEARCH OF TARGET**  
**COMPUTERS**

27. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of premises for information that might be stored on digital devices or other electronic storage media often requires the seizure of the physical items and later off-site review consistent with the warrant. In lieu of removing all of these items from the premises, it is sometimes possible to make an image copy of the data on the digital devices or other electronic storage media, onsite. Generally speaking, imaging is the taking of a complete electronic picture of the device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the item, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine the respective digital device and/or electronic storage media to obtain evidence. Computer hard drives, digital devices and electronic storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements.* Digital devices or other electronic storage media can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the items off-site and reviewing them in a controlled environment will allow examination with the proper tools and knowledge.

c. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of electronic storage media formats and on a

1 variety of digital devices that may require off-site reviewing with specialized  
2 forensic tools.

### 3 SEARCH TECHNIQUES

4 28. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal  
5 Rules of Criminal Procedure, the warrant I am applying for will permit seizing, imaging,  
6 or otherwise copying digital devices or other electronic storage media that reasonably  
7 appear capable of containing some or all of the data or items that fall within the scope of  
8 Attachment B to this Affidavit, and will specifically authorize a later review of the media  
9 or information consistent with the warrant.

10 29. Because others have been identified as residents at the SUBJECT  
11 PREMISES, it is possible that the SUBJECT PREMISES will contain digital devices or  
12 other electronic storage media that are predominantly used, and perhaps owned, by  
13 persons who are not suspected of a crime. If agents conducting the search nonetheless  
14 reasonably determine that it is possible that the things described in this warrant could be  
15 found on those computers, this application seeks permission to search and if necessary to  
16 seize those computers as well. It may be impossible to determine, on scene, which  
17 computers contain the things described in this warrant.

18 30. Consistent with the above, I hereby request the Court's permission to seize  
19 and/or obtain a forensic image of digital devices or other electronic storage media that  
20 reasonably appear capable of containing data or items that fall within the scope of  
21 Attachment B to this Affidavit, and to conduct off-site searches of the digital devices or  
22 other electronic storage media and/or forensic images, using the following procedures:

#### 23 **A. Processing the Search Sites and Securing the Data.**

24 a. Upon securing the physical search site, the search team will conduct an  
25 initial review of any digital devices or other electronic storage media located at  
26 the subject premises described in Attachment A that are capable of containing  
27 data or items that fall within the scope of Attachment B to this Affidavit, to  
determine if it is possible to secure the data contained on these devices onsite

1 in a reasonable amount of time and without jeopardizing the ability to  
2 accurately preserve the data.

3 b. In order to examine the electronically stored information (“ESI”) in a  
4 forensically sound manner, law enforcement personnel with appropriate  
5 expertise will attempt to produce a complete forensic image, if possible and  
6 appropriate, of any digital device or other electronic storage media that is  
7 capable of containing data or items that fall within the scope of Attachment B  
8 to this Affidavit.<sup>5</sup>

9 c. A forensic image may be created of either a physical drive or a logical  
10 drive. A physical drive is the actual physical hard drive that may be found in a  
11 typical computer. When law enforcement creates a forensic image of a  
12 physical drive, the image will contain every bit and byte on the physical drive.  
13 A logical drive, also known as a partition, is a dedicated area on a physical  
14 drive that may have a drive letter assigned (for example the c: and d: drives on  
15 a computer that actually contains only one physical hard drive). Therefore,  
16 creating an image of a logical drive does not include every bit and byte on the  
17 physical drive. Law enforcement will only create an image of physical or  
18 logical drives physically present on or within the subject device. Creating an  
19 image of the devices located at the search locations described in Attachment A  
20 will not result in access to any data physically located elsewhere. However,  
21 digital devices or other electronic storage media at the search locations  
22 described in Attachment A that have previously connected to devices at other  
23 locations may contain data from those other locations.

24 d. If based on their training and experience, and the resources available to  
25 them at the search site, the search team determines it is not practical to make an  
26 on-site image within a reasonable amount of time and without jeopardizing the  
27 ability to accurately preserve the data, then the digital devices or other  
electronic storage media will be seized and transported to an appropriate law  
enforcement laboratory to be forensically imaged and reviewed.

## 21 **B. Searching the Forensic Images.**

---

23 <sup>5</sup> The purpose of using specially trained computer forensic examiners to conduct the imaging of digital devices or  
24 other electronic storage media is to ensure the integrity of the evidence and to follow proper, forensically sound,  
25 scientific procedures. When the investigative agent is a trained computer forensic examiner, it is not always  
26 necessary to separate these duties. Computer forensic examiners often work closely with investigative personnel to  
27 assist investigators in their search for digital evidence. Computer forensic examiners are needed because they  
generally have technological expertise that investigative agents do not possess. Computer forensic examiners,  
however, often lack the factual and investigative expertise that an investigative agent may possess on any given  
case. Therefore, it is often important that computer forensic examiners and investigative personnel work closely  
together.

1 a. Searching the forensic images for the items described in Attachment B may  
 2 require a range of data analysis techniques. In some cases, it is possible for  
 3 agents and analysts to conduct carefully targeted searches that can locate  
 4 evidence without requiring a time-consuming manual search through unrelated  
 5 materials that may be commingled with criminal evidence. In other cases,  
 6 however, such techniques may not yield the evidence described in the warrant,  
 7 and law enforcement may need to conduct more extensive searches to locate  
 8 evidence that falls within the scope of the warrant. The search techniques that  
 9 will be used will be only those methodologies, techniques and protocols as  
 10 may reasonably be expected to find, identify, segregate and/or duplicate the  
 11 items authorized to be seized pursuant to Attachment B to this affidavit. Those  
 12 techniques, however, may necessarily expose many or all parts of a hard drive  
 13 to human inspection in order to determine whether it contains evidence  
 14 described by the warrant.

15 b. These methodologies, techniques and protocols may include the use of a  
 16 “hash value” library to exclude normal operating system files that do not need  
 17 to be further searched. OR - Agents may utilize hash values to exclude certain  
 18 known files, such as the operating system and other routine software, from the  
 19 search results.

### BIOMETRIC UNLOCK

20 31. The warrant I am applying for would permit law enforcement to obtain  
 21 from certain individuals the display of physical biometric characteristics (such as  
 22 fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to  
 23 search and seizure pursuant to this warrant. I seek this authority based on the following:

24 a. I know from my training and experience, as well as from  
 25 information found in publicly available materials published by device  
 26 manufacturers, that many electronic devices, particularly newer mobile devices  
 27 and laptops, offer their users the ability to unlock the device through biometric  
 features in lieu of a numeric or alphanumeric passcode or password. These  
 biometric features include fingerprint scanners and facial recognition features.  
 Some devices offer a combination of these biometric features, and the user of such  
 devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable  
 the ability to unlock the device through his or her fingerprints. For example, Apple  
 offers a feature called “Touch ID,” which allows a user to register up to five  
 fingerprints that can unlock a device. Once a fingerprint is registered, a user can  
 unlock the device by pressing the relevant finger to the device’s Touch ID sensor,

1 which is found in the round button (often referred to as the “home” button) located  
2 at the bottom center of the front of the device. The fingerprint sensors found on  
3 devices produced by other manufacturers have different names but operate  
4 similarly to Touch ID.

5 c. If a device is equipped with a facial recognition feature, a user may  
6 enable the ability to unlock the device through his or her face, iris, or retina. For  
7 example, Apple offers a facial recognition feature called “Face ID.” During the  
8 Face ID registration process, the user holds the device in front of his or her face.  
9 The device’s camera then analyzes and records data based on the user’s facial  
10 characteristics. The device can then be unlocked if the camera detects a face with  
11 characteristics that match those of the registered face. Facial recognition features  
12 found on devices produced by other manufacturers have different names but  
13 operate similarly to Face ID.

14 d. While not as prolific on digital devices as fingerprint and facial-  
15 recognition features, both iris and retina scanning features exist for securing  
16 devices/data. The human iris, like a fingerprint, contains complex patterns that are  
17 unique and stable. Iris recognition technology uses mathematical pattern-  
18 recognition techniques to map the iris using infrared light. Similarly, retina  
19 scanning casts infrared light into a person’s eye to map the unique variations of a  
20 person’s retinal blood vessels. A user can register one or both eyes to be used to  
21 unlock a device with these features. To activate the feature, the user holds the  
22 device in front of his or her face while the device directs an infrared light toward  
23 the user’s face and activates an infrared sensitive camera to record data from the  
24 person’s eyes. The device is then unlocked if the camera detects the registered eye.

25 e. In my training and experience, users of electronic devices often  
26 enable the aforementioned biometric features because they are considered to be a  
27 more convenient way to unlock a device than by entering a numeric or  
alphanumeric passcode or password. Moreover, in some instances, biometric  
features are considered to be a more secure way to protect a device’s contents.  
This is particularly true when the users of a device are engaged in criminal  
activities and thus have a heightened concern about securing the contents of a  
device.

28 f. As discussed in this affidavit, based on my training and experience I  
29 believe that one or more digital devices will be found during the search. The  
30 passcode or password that would unlock the device(s) subject to search under this  
31 warrant is not known to law enforcement. Thus, law enforcement personnel may  
32 not otherwise be able to access the data contained within the device(s), making the  
33 use of biometric features necessary to the execution of the search authorized by  
34 this warrant.

1 g. I also know from my training and experience, as well as from  
2 information found in publicly available materials including those published by  
3 device manufacturers, that biometric features will not unlock a device in some  
4 circumstances even if such features are enabled. This can occur when a device has  
5 been restarted, inactive, or has not been unlocked for a certain period of time. For  
6 example, Apple devices cannot be unlocked using Touch ID when (1) more than  
7 48 hours has elapsed since the device was last unlocked or (2) when the device has  
8 not been unlocked using a fingerprint for 4 hours *and* the passcode or password  
9 has not been entered in the last 156 hours. Biometric features from other brands  
10 carry similar restrictions. Thus, in the event law enforcement personnel encounter  
11 a locked device equipped with biometric features, the opportunity to unlock the  
12 device through a biometric feature may exist for only a short time.

13 h. In my training and experience, the person who is in possession of a  
14 device or has the device among his or her belongings at the time the device is  
15 found is likely a user of the device. However, in my training and experience, that  
16 person may not be the only user of the device, and may not be the only individual  
17 whose physical characteristics are among those that will unlock the device via  
18 biometric features. Furthermore, while physical proximity is an important factor  
19 in determining who is the user of a device, it is only one among many other factors  
20 that may exist.

21 32. Due to the foregoing, I request that if law enforcement personnel encounter  
22 a device that is subject to search and seizure pursuant to this warrant and may be  
23 unlocked using one of the aforementioned biometric features, and if law enforcement  
24 reasonably suspects the SUBJECT PERSON is a user of the device, then – for the  
25 purpose of attempting to unlock the device in order to search the contents as authorized  
26 by this warrant – law enforcement personnel shall be authorized to: (1) press or swipe the  
27 fingers (including thumbs) of such person to the fingerprint scanner of the device; and/or  
28 (2) hold the device in front of the face and open eyes of such person and activate the  
29 facial, iris, or retina recognition feature.

30 33. In pressing or swiping an individual's thumb or finger onto a device and in  
31 holding a device in front of an individual's face and open eyes, law enforcement may not  
32 use excessive force, as defined in *Graham v. Connor*, 490 U.S. 386 (1989); specifically,  
33 law enforcement may use no more than objectively reasonable force in light of the facts  
34 and circumstances confronting them.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27

Affidavit of SA Kyle McNeal - 22  
USAO# 2025R00489

UNITED STATES ATTORNEY  
700 STEWART STREET, SUITE 5220  
SEATTLE, WASHINGTON 98101-1271  
206-553-2279

**CONCLUSION**

34. Based on the foregoing, I believe there is probable cause to conclude that evidence, fruits, and instrumentalities of the TARGET OFFENSES will be found during a search of the SUBJECT PREMISES/PERSON/VEHICLES, as more fully described in Attachment A to this Affidavit, as well as on and in any digital devices or other electronic storage media found. I therefore request that the court issue a warrant authorizing a search of the SUBJECT PREMISES/PERSON/VEHICLES, as well as any digital devices and electronic storage media located therein, for the items more fully described in Attachment B.

35. The affidavit and application are being presented by reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41(d)(3).

*Kyle McNeal*

Kyle McNeal  
Special Agent

The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit this 11th day of April, 2025.

  
GRADY J. LEUPOLD  
United States Magistrate Judge

**ATTACHMENT A**

The SUBJECT PREMISES is the property located at 5944 N 12<sup>th</sup> Street, Joint Base Lewis-Chord (JBLM), Washington 98433, that contains a single-family home with attached garage, see images below.



The search is to include the entirety of the residence and any garages or outbuildings located on the SUBJECT PREMISES, and any digital device(s) or other electronic storage media found.

1 The SUBJECT PERSON is James Andrew Davis (DOB: XX/XX/1991)  
2 pictured below:



13  
14  
15 The search is to include the SUBJECT PERSON and any backpacks, bags, or  
16 closed containers being carried by the SUBJECT PERSON, as well as any digital  
17 devices or electronic storage media found.  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27

1       SUBJECT VEHICLE 1 is a 1986 Chevrolet Blazer bearing Washington Plate:  
2       CGN9993

3       SUBJECT VEHICLE 2 is a 2015 Kia Sportage, bearing Washington Plate:  
4       BMH3641.

5       The search is to include the entirety of the SUBJECT VEHICLES and any  
6       compartments or closed containers, as well as any digital devices or electronic storage  
7       media found.

**ATTACHMENT B**

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed); photocopies or other photographic form; and electrical, electronic, and magnetic form (such as tapes, cassettes, hard disks, floppy disks, diskettes, compact discs, CD-ROMs, DVDs, optical discs, Zip cartridges, printer buffers, smart cards, or electronic notebooks, or any other electronic storage medium) that constitute evidence, instrumentalities, or fruits of violations or attempted violations of 18 U.S.C. § 2251(a), (e) (Production of Child Pornography, 18 U.S.C. 2252(a)(2), (b)(1) (Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B), (b)(2) (Possession of Child Pornography) (the TARGET OFFENSES):

1. Documents, records, and things that constitute evidence of who exercises dominion and control over the SUBJECT PREMISES.
2. All records relating to violations of the TARGET OFFENSES, including:
  - a. visual depictions of minors engaged in sexually explicit conduct
  - b. identifying information for any individuals shown in such depictions or evidence that would otherwise assist in the identification of those depicted or those responsible for creating such visual depictions
  - c. information concerning the possession, receipt, distribution, or production of visual depictions of minors engaged in sexually explicit conduct
  - d. information identifying the source of any visual depictions of minors engaged in sexually explicit conduct
  - e. evidence of communications related to the possession, receipt, distribution, or production of visual depictions of minors engaged in sexually explicit conduct
  - f. evidence of contact with or communications about minors
  - g. evidence indicative of a sexualized interest in minors or depictions of minors

3. Digital devices<sup>6</sup> or other electronic storage media<sup>7</sup> and/or their components, which include:

a. Any digital device or other electronic storage media capable of being used to commit, further, or store evidence of the offenses listed above;

b. Any digital devices or other electronic storage media used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, plotters, encryption devices, and optical scanners;

c. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or other electronic storage media or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

4. For any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be contained, or that may contain things otherwise called for by this warrant:

---

<sup>6</sup> “Digital device” includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants (“PDAs”), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

<sup>7</sup> Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

1 a. evidence of who used, owned, or controlled the digital device or  
2 other electronic storage media at the time the things described in this warrant were  
3 created, edited, or deleted, such as logs, registry entries, configuration files, saved  
4 usernames and passwords, documents, browsing history, user profiles, email, email  
5 contacts, "chat," instant messaging logs, photographs, and correspondence;

6 b. evidence indicating how and when the computer was accessed or  
7 used to determine the chronological context of computer access, use, and events relating  
8 to the crime(s) under investigation and to the computer user;

9 c. evidence of software that would allow others to control the digital  
10 device or other electronic storage media, such as viruses, Trojan horses, and other forms  
11 of malicious software, as well as evidence of the presence or absence of security software  
12 designed to detect malicious software;

13 d. evidence of the lack of such malicious software;

14 e. evidence of the attachment to the digital device of other storage  
15 devices or similar containers for electronic evidence;

16 f. evidence of counter-forensic programs (and associated data) that are  
17 designed to eliminate data from the digital device or other electronic storage media;

18 g. evidence of the times the digital device or other electronic storage  
19 media was used;

20 h. passwords, encryption keys, and other access devices that may be  
21 necessary to access the digital device or other electronic storage media;

22 i. documentation and manuals that may be necessary to access the  
23 digital device or other electronic storage media or to conduct a forensic examination of  
24 the digital device or other electronic storage media;

25 j. contextual information necessary to understand the evidence  
26 described in this attachment.

27 5. Records and things evidencing the use of the internet, including:

a. routers, modems, and network equipment used to connect computers  
to the Internet;

b. records of Internet Protocol addresses used;

1 c. records of Internet activity, including firewall logs, caches, browser  
2 history and cookies, “bookmarked” or “favorite” web pages, search terms that the user  
3 entered into any Internet search engine, and records of user-typed web addresses.

4 6. During the execution of the search of the SUBJECT  
5 PREMISES/PERSON/VEHICLES described in Attachment A, if law enforcement  
6 encounters a smartphone or other electronic device equipped with a biometric-unlock  
7 feature, and if law enforcement reasonably suspects the SUBJECT PERSON is a user of  
8 the device, then – for the purpose of attempting to unlock the device in order to search the  
9 contents as authorized by this warrant – law enforcement personnel are authorized to: (1)  
10 press or swipe the fingers (including thumbs) of such person to the fingerprint scanner of  
11 the device; and/or (2) hold the device in front of the face and open eyes of such person  
12 and activate the facial, iris, or retina recognition feature.

13 7. In pressing or swiping an individual’s thumb or finger onto a device and in  
14 holding a device in front of an individual’s face and open eyes, law enforcement may not  
15 use excessive force, as defined in *Graham v. Connor*, 490 U.S. 386 (1989); specifically,  
16 law enforcement may use no more than objectively reasonable force in light of the facts  
17 and circumstances confronting them.

18  
19 THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE  
20 MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS  
21 SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO  
22 THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC  
23 STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL  
24 ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE  
25 CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR  
26  
27

1 EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED  
2 CRIMES